ITS
Office of Information Technology Services

Security Assessment Project

Agency Briefing

September 25 and 30, 2003

NC your service
www.ncgov.com

Office of Information Technology Services

Agenda

Topic	Presenter	Time (min)
Welcome/Introductions/ Comments	Ann Garrett, Chief Security Officer	10
Project Overview	Ruth Steinberg, V.P., Gartner	60
Questions	Participants	30
Next Steps	Ann Garrett	10
Adjournment – Total Minutes		**110**

Agency Security Liaisons are required check in and pick up Agency Preparation Communications Package

Office of Information Technology Services

Project Background - Security Legislation

- Compliance with Section 1.(a) G.S. 147-33.82, Section 1.(a) is amended by adding a new section to read:"(e1) The State Chief Information Officer shall assess the ability of each agency to comply with the current security enterprise-wide set of standards established pursuant to this section. The assessment shall include, at a minimum, the rate of compliance with the standards in each agency and an assessment of each agency's security organization, network security architecture, and current expenditures for information technology security. The assessment shall also estimate the cost to implement the security measures needed for agencies to fully comply with the standards. Each agency subject to the standards shall submit information required by the State Chief Information Officer for purposes of this assessment. Not later than May 4, 2004, the Information Resources Management Commission and the State Chief Information Officer shall submit a public report that summarizes the status of the assessment, including the available estimates of additional funding needed to bring agencies into compliance, to the Joint Legislative Commission on Governmental Operations and shall provide updated assessment information by January 15 of each subsequent year."

Project Background - Security Legislation

- The State CIO shall assess the ability of each agency to comply with the current security enterprise-wide set of standards established
- The assessment shall include, at a minimum,
  - the rate of compliance with the standards in each agency
  - an assessment of each agency's security organization, network security architecture
  - current expenditures for information technology security.
  - cost to implement the security measures needed for agencies to fully comply with the standards.
- Each agency subject to the standards shall submit information required by the State CIO for purposes of this assessment.
- Not later than May 4, 2004, the IRMC and the State CIO shall submit a public report to the Joint Legislative Commission on Governmental Operations, that
  - summarizes the status of the assessment
  - includes estimates of additional funding needed to bring agencies into compliance
- The IRMC and State CIO shall provide updated assessment information by January 15 of each subsequent year.

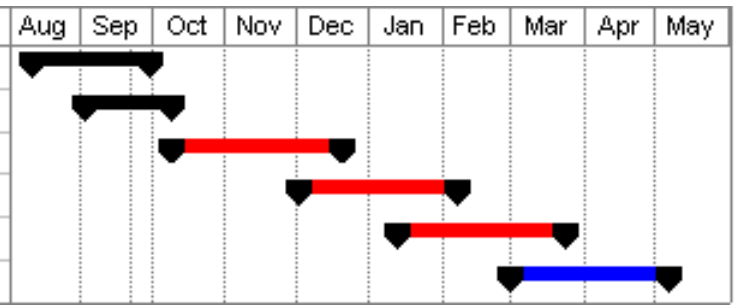
Office of Information Technology Services

Project Background - Timeline

- Security assessment project is 4-phase process.
- Phases 1 and 2 consist of preparation by the Project Management Office (PMO)
- Phase 3: Security assessments will be conducted in 3 Groups:
  - Group 1 - October 13 – December 4
  - Group 2 - December 2 – February 3
  - Group 3A - January 12 – March 24
  - Group 3B - January 28 – March 24

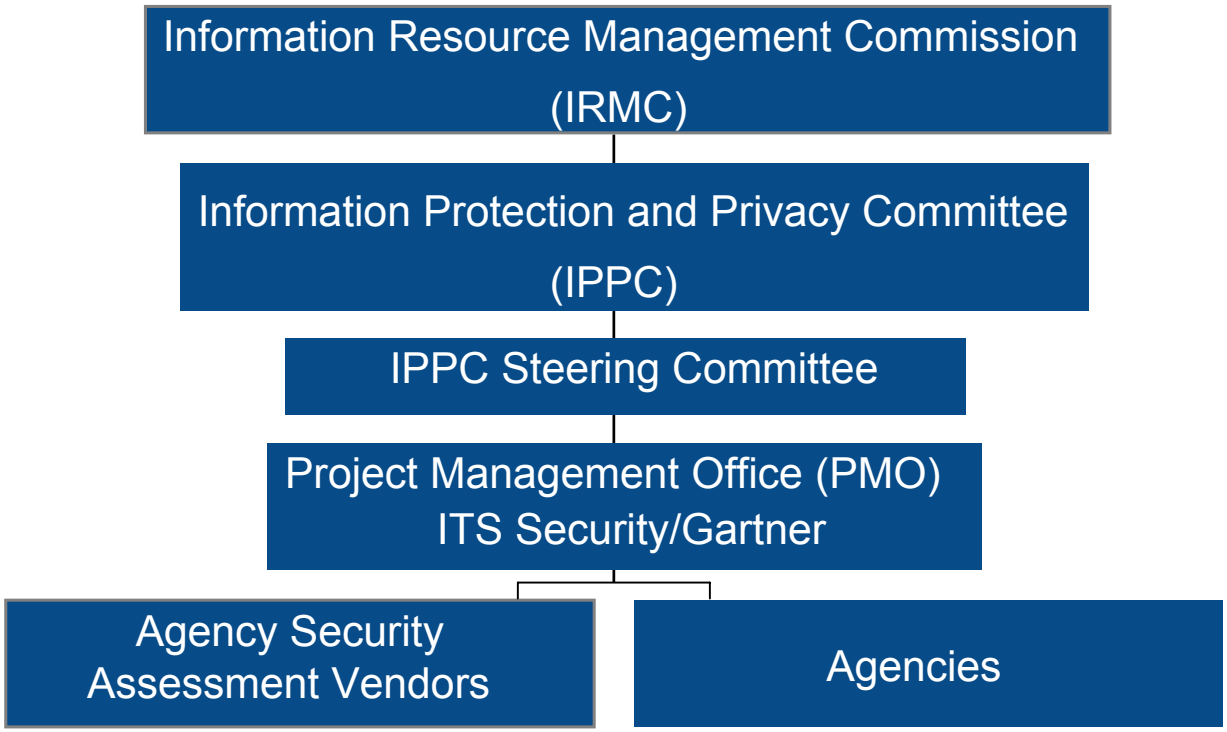
  PMO prepares preliminary findings and extrapolated estimates beginning Dec.
- Phase 4 - PMO identifies statewide security risks and develops cost and resource estimate for statewide corrective action.

ID	Task Name
1	**Phase 1 - Organize Project Management Office**
2	**Phase 2 - Assessment Preparation**
3	**Phase 3 - Conduct Security Assessments (Group 1)**
4	**Phase 3 - Conduct Security Assessments (Group 2)**
5	**Phase 3 - Conduct Security Assessments (Group 3)**
6	**Phase 4 - Develop Final Report**



Office of Information Technology Services

Security Project Reporting Structure



Office of Information Technology Services

Project Responsibilities

Participants	Primary Responsibilities
Project Management Office – ITS / Gartner	• Develop all project tools and templates • Manage assessment project • Develop preliminary and extrapolated cost estimates • Develop final recommendations and final cost estimates • Train vendors in use of tools and templates • Project reporting
Vendors	• Conduct assessments of assigned agencies • Project Management/Reporting to PMO (status, issues, etc.)
Agencies	• Led by agency security liaison • Prepare for assessments • Provide documentation • Participate in assessments

Office of Information Technology Services

Project Team Introductions

- **ITS Team Members**
  - Ann Garrett, Project Sponsor
  - Charles “Chip” Moore, Security Analyst
  - Julean Self, Planning Analyst
  - Christopher “Chris” Turpin, Security Analyst
- **Gartner Team Members**
  - Nazmin Alani, Project Team Member
  - John Dubiel, Subject Matter Expert
  - Daniel Saroff, Subject Matter Expert
  - Elizabeth Sernoff, Project Team Member
  - Ruth Steinberg, Engagement Manager
  - Lance Westerlund, Project Office Manager

Office of Information Technology Services

Agenda Revisited

Topic	Presenter	Time (min)
Welcome/Introductions/ Comments	Ann Garrett, Chief Security Officer	10
Project Overview	Ruth Steinberg, V.P., Gartner	60
Questions	Participants	30
Next Steps	Ann Garrett	10
Adjournment – Total Minutes		**110**

Office of Information Technology Services

Security Assessment Project Overview

- Project Background
- Approach and Methodology
- Agency Responsibilities
- Critical Success Factors
- Schedule
- Next Steps and Questions?

Project Background - Response

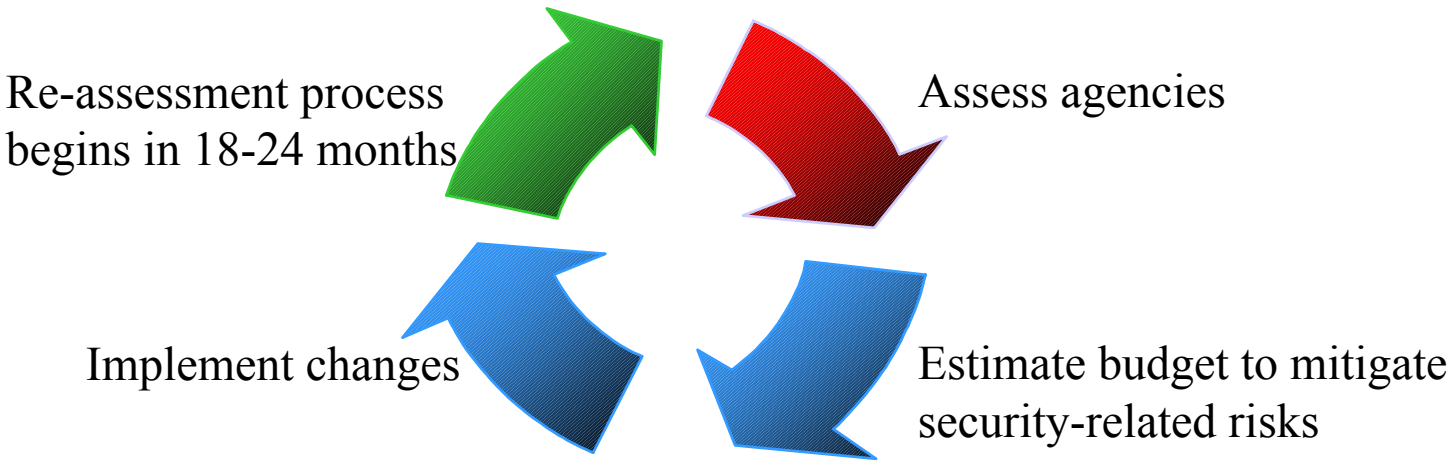
- In response to provisions North Carolina Session Law 2003-153, which states that periodic agency security assessments will be performed by the State Chief Information Officer (SCIO), the State of North Carolina has initiated a statewide security assessment of all Executive Branch agencies.
- Assessment process is intended to provide key-decision makers with:
  - Global view of the security status of agencies
  - Detailed findings sufficient to permit State to prioritize and budget for required remediation efforts.
- Assessment will be based on the North Carolina Security Policy which is based on ISO17799 standard.

Documents Overview

- Requirements Document - overview of project goals, assessment process, and roles and responsibilities
- Agency Preparation Communications Package - additional guidance to agencies covering:
  - Agency preparation activities and tools
  - Requested documentation
  - Agency interview guidelines
    - Selection guidance
    - Interview preparation
    - Scheduling template

Assessment Process Definition

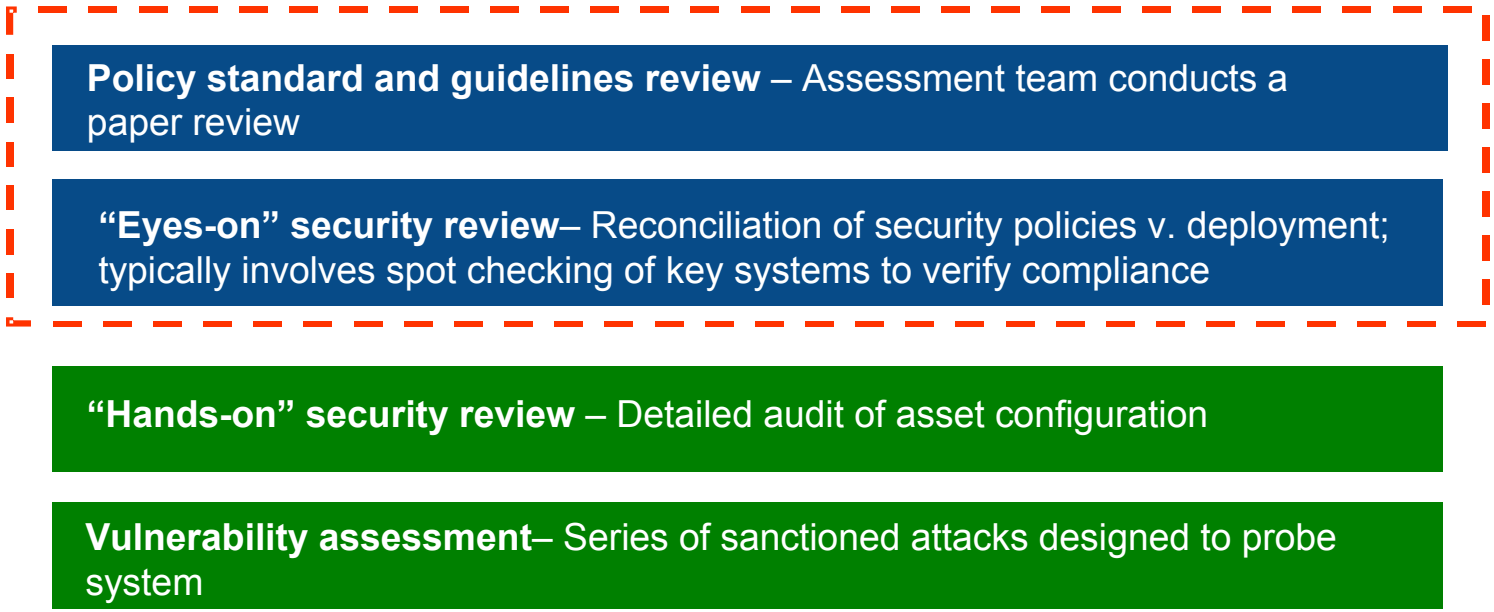
- A process of defining, selecting, designing, collecting, analyzing, interpreting, and using information for the purpose of determining how well performance matches baseline standards and expectations.



Office of Information Technology Services

Approach & Methodology - The "What"

- There are four ways to capture security information. The State's Security Assessment Project will use the first two.



Office of Information Technology Services

Approach & Methodology -
Assessment Focus Areas

Security Policy	Management support, commitment, direction in accomplishing information security goals
Organizational Security	Need for management framework that creates, sustains, and manages security infrastructure of organization
Asset Classification and Control	Ability of security infrastructure to protect organizational assets
Personnel Security	Organization's ability to mitigate risk inherent in human interactions
Physical Security	Risk inherent to organizational premises
Communications & Operations	Organization's ability to ensure correct and secure operation of its assets

Approach & Methodology -
Assessment Focus Areas

Access Administration	Organization's ability to administratively control access to assets based on business and security requirements
Access Technology	Organization's ability to control access to technology-specific assets based on business and security requirements
Applications Development & Maintenance	Organization's ability to ensure appropriate information system security controls are incorporated and maintained
Business Impact / Continuity	Organization's ability to counteract interruptions to normal operations
Compliance	Organization's ability to remain in compliance with regulatory, statutory, contractual and security requirements.

Office of Information Technology Services

Approach & Methodology -
Scope of the Assessment

	100: Info Security Project Charter	110: Security Policy	120: Organizational Security	130: Asset ID & Classification	140: Personnel Security	150: Physical & Enviro Security	160: Comms & Ops Management	170: Access Control	180: Systems Dev & Maintenance	190: Business Continuity Mgmt	200: Compliance
People											
Agency / IT Management	◆	◆	◆		◆	◆	◆			◆	◆
Insourced	◆	◆	◆		◆	◆	◆			◆	◆
Outsourced Services (e.g. off site)	◆	◆	◆		◆	◆	◆			◆	◆
Out-tasked Services (e.g. on site)	◆	◆	◆		◆	◆	◆			◆	◆
Hardware											
Mainframe		◆		◆		◆		◆	◆	◆	◆
Midrange		◆		◆		◆		◆	◆	◆	◆
NAS / SAN		◆		◆		◆		◆	◆	◆	◆
Desktops		◆		◆		◆		◆	◆	◆	◆
Laptops		◆		◆		◆		◆	◆	◆	◆
PDAs		◆		◆							◆

Excerpt from the Scope section of the Requirements Document

Office of Information Technology Services

Approach & Methodology - Security Assessment Tool

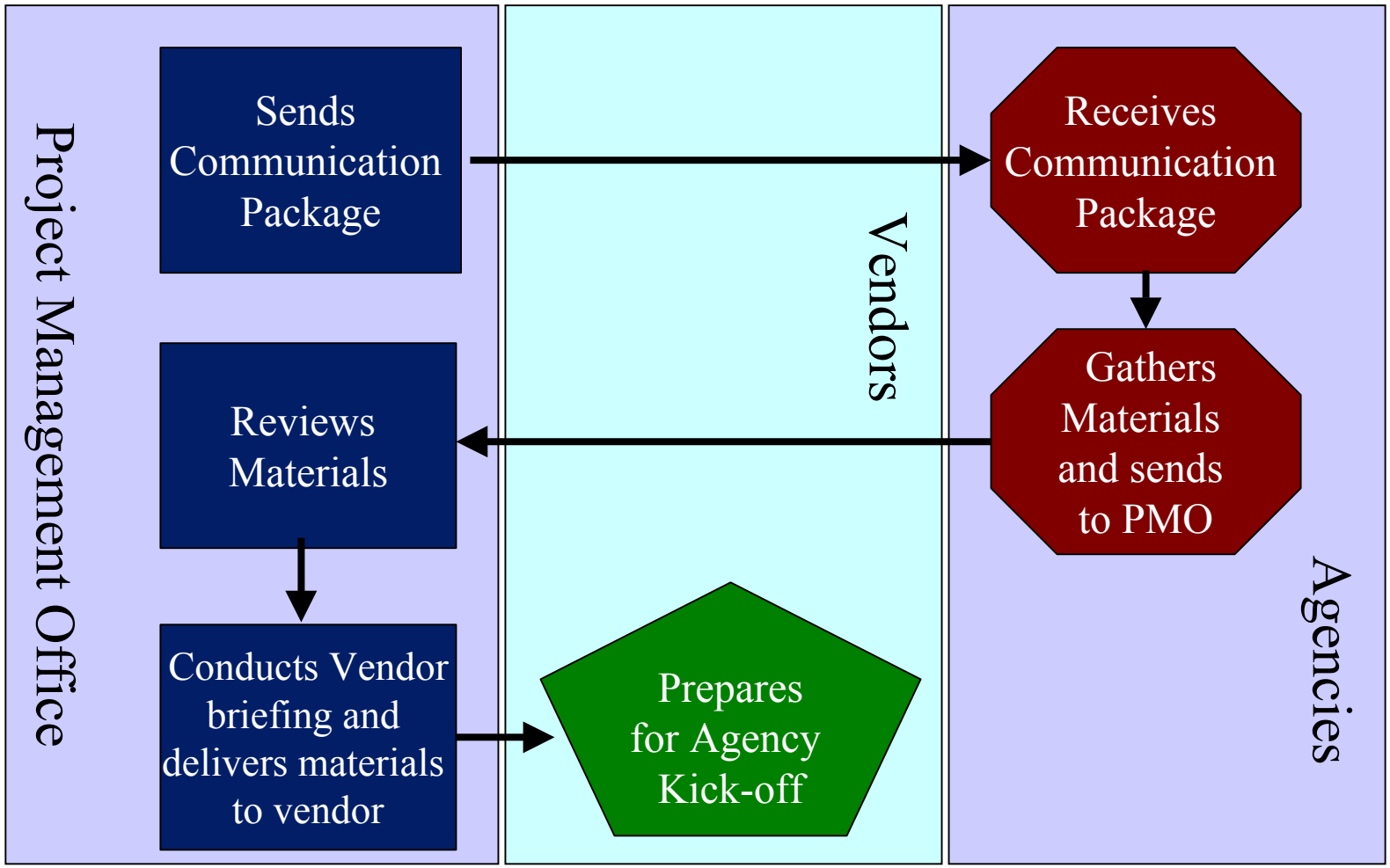
- The vendor works with the agencies to complete the tool.

1.1	Security Policies, Standards, & Procedures	Quality 1=Best Practice 2=Meets Reqs 3=Deficient 4=Unacceptable	Execution 1=Fully 2=Critical Areas 3=Minimal/Gaps 4=None/WIP	Justification	Documentation
1.1.1	Is there an agency security PSP in place?				
1.1.2	Does the PSP state what is and is not permissible?				
1.1.3	Is the agency PSP in compliance with State Security PSPs?				
1.1.4	Have the State PSPs been augmented to reflect unique agency requirements?				
1.1.5	Does the scope of the PSP cover all facets of information?				
1.1.6	Does the PSP define and identify what is classed as information?				

Excerpt from the Security Policies, Standards, and Procedures section of security assessment tool

Office of Information Technology Services

Phase 2: Pre-Assessment Process



Types of Agency Data

- Five (5) business days prior to scheduled assessment kick-off date, Agency sends the following types of information:
  - Contact Information List of staff members to be interviewed with a proposed interview schedule
  - Checklist of documentation for review by vendors
- Intent is to familiarize vendor with agency's organizational structure, security policies and procedures, etc.
- Once vendor is on site, additional information is collected during meetings, interviews, etc.
- Specific guidance as to what documentation is required is contained in Agency Preparation Communications Package.

Phase 3: Security Assessments

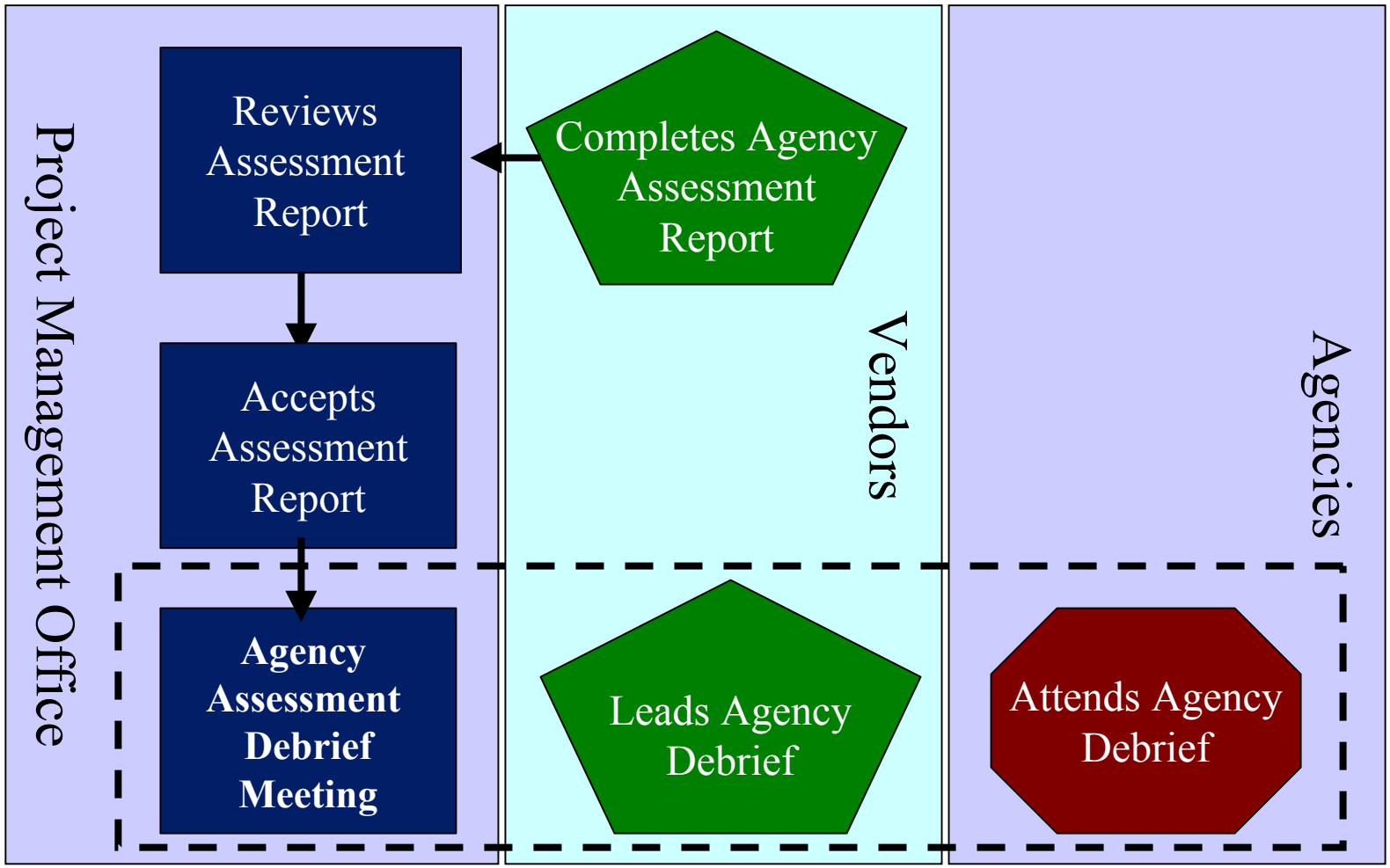
- Interviews with key personnel
- Review of Detailed Documents in support of Policies
- Vendor observations at the Agency

Interview Guidelines

- Vendors need to speak with the following types of staff:
  - IT Management
  - Agency security liaison
  - Physical security team
  - Networking / Operations staff
  - Human resources and/or individual(s) responsible for employee background checks
  - Business Continuity Manager / Lead
  - Other technical resources, as appropriate
- Same staff would normally attend vendor kickoff and agency debrief meetings.

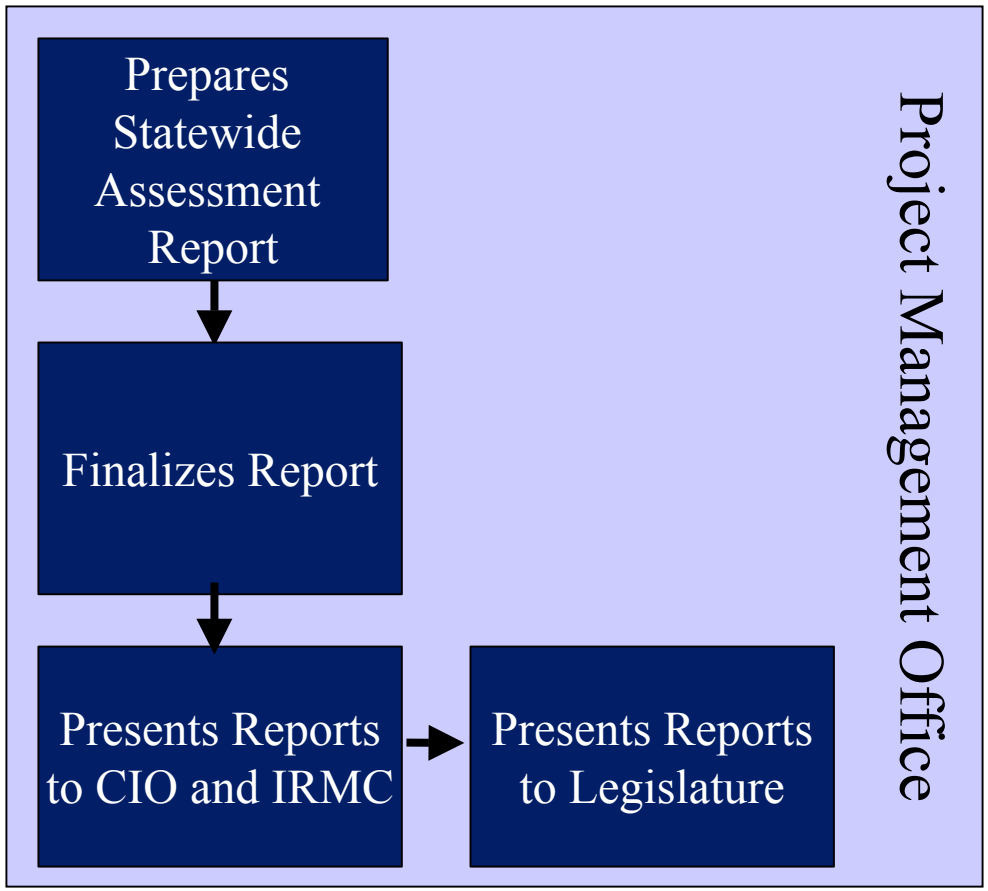
Office of Information Technology Services

Phase 3: Agency Closeout Process



Office of Information Technology Services

Phase 4: Enterprise Security Assessment Results



Office of Information Technology Services

Critical Success Factors

- Agencies dedicate adequate resources toward effort
- All participants properly prepare for Assessment
- Roles and responsibilities for all participating parties clearly understood
- All participants adhere to project schedule and budget
- Risks identified, documented and mitigated promptly and openly
- Communication remains open and honest.

There are no additional resources available to allow for time or budget overruns

Office of Information Technology Services

Schedule

Activity/Deadline	Date	Notes
Vendor Bid Responses Due	Sept. 3	Completed
Vendor Selection Complete	Sept. 15	Completed
Agency Project Overview Briefing (Session 1)	Sept. 25	1:30pm-3:30pm Department of Cultural Resources Auditorium
Agency Project Overview Briefing (Session 2)	Sept. 30	2pm-4pm Department of Cultural Resources Auditorium
Vendor Assessment Training	Oct. 8	1pm-5pm Department of Cultural Resources Auditorium
Security Assessment Report Due	May 4	

Assessment Activity	Start Date	End Date	Notes
Agency Assessment - Group 1	Oct. 13	Dec. 4	At agency location
Agency Assessment - Group 2	Dec. 2	Feb. 3	At agency location
Agency Assessment - Group 3A	Jan. 12	March 24	At agency location
Agency Assessment - Group 3B	Jan. 28	March 24	At agency location

Office of Information Technology Services

Agency Assessment Tracks
Group 1

Agency	Start	End
Secretary of State	10/13/03	12/1/03
Labor	10/13/03	12/1/03
Auditor	10/13/03	12/1/03
Administration	10/13/03	12/1/03
Environment & Natural Resources	10/13/03	12/1/03
ITS	10/13/03	12/1/03
Health & Human Services	10/13/03	12/4/03
Dept of Transportation	10/13/03	12/4/03
Corrections	10/13/03	12/4/03

Office of Information Technology Services

Agency Assessment Tracks
Group 2

Agency	Start	End
Public Instruction	12/2/03	1/27/04
Dept of Insurance	12/2/03	1/27/04
Community College System	12/2/03	1/27/04
Dept of Juvenile Justice	12/2/03	2/3/04
Dept of Crime Control	12/2/03	2/3/04
Department of Commerce	12/2/03	2/3/04
Department of Agriculture	12/2/03	2/3/04

Office of Information Technology Services

Agency Assessment Tracks
Group 3

Agency	Start	End
Office of the Governor	2/4/04	3/17/04
Office of the Lt. Governor	2/4/04	3/17/04
Office of State Personnel	1/12/04	2/23/04
Office of State Budget and Mgmt	2/4/04	3/17/04
Department of Cultural Resources	2/4/04	3/17/04
Office of State Controller	1/12/04	3/1/04
Employment Security Commission	1/28/04	3/17/04
Dept of Justice	1/28/04	3/17/04
Department of State Treasurer	2/4/04	3/24/04
Department of Revenue	1/12/04	3/1/04

Next Steps

Identify Interviewees
Scheduling Interview
Collect Data and Documentation

Questions?

Office of Information Technology Services

PMO Contact

Christopher “Chris” Turpin
(919) 981-2549
security.pmo@ncmail.net

All hard copy documentation must be sent to the following mailbox:
Chris Turpin, ITS
Mail Courier 51-01-11